Here's a detailed summary of this NY Times story via Claude AI:
https://www.nytimes.com/2026/05/23/world/europe/phone-theft-threats-london.html

---

The Theft

Alex Pikula, a 37-year-old from Chicago visiting London, had his iPhone snatched by an e-bike rider as he left a theater in the West End — a crime that has become alarmingly common in the British capital. He reported it to police, but knew the odds of recovery were slim. He figured it was frustrating but over. He was wrong.

The Escalating Threats

Because his mother Judi Pikula's number was listed as the contact in his phone's "lost mode," she became the unwitting target of a sophisticated, multi-stage intimidation campaign:

1. **Stage 1 – Deception:** A text appeared to come from Apple Pay, warning that someone was trying to use the phone in China and that the Apple ID needed to be unlinked to protect her son's financial accounts. It was a fake.
2. **Stage 2 – The "Friendly Stranger":** A chirpy message arrived from a number with a Philippines country code, starting with "Yo!!" The sender claimed to have recently bought the phone and could see Alex's messages, emails, bank details, notes, and personal information. Detailed instructions for unlinking the Apple ID were included.
3. **Stage 3 – Threats of Auction:** Another message, also apparently from the Philippines, warned that the phone would be "auctioned on the black market" along with all of Alex's personal data.
4. **Stage 4 – Violent Threats:** When Judi tried to ignore the messages, a video arrived of a man brandishing a gun, accompanied by messages threatening sexual assault, death, and that her family would be "slaughtered." One message read: *"I know who you are and where you live. I've killed for far less than a phone before."*

The Family's Response

Alex initially told his mother to ignore the messages, doubting their credibility — especially since the Find My app showed his phone in Shenzhen, China, a known destination for stolen iPhones. But Judi, 65, was genuinely frightened. Even though she suspected the threats were hollow, she couldn't be sure. After the gun video arrived, she was, in her words, "freaking out."

Ultimately, Alex decided to give in. He wiped the phone and unlinked it from his Apple ID — exactly what the criminals wanted. The messages to his mother stopped immediately.

How Widespread Is This?

The article makes clear this is not an isolated incident. London had a record **81,000 phones reported stolen in 2024**, dropping to about 71,000 in 2025. The Metropolitan Police have identified international

criminal networks shipping stolen phones to China, where they're sold on the black market — but only if they can be reset, which requires unlinking the Apple ID. Without that, a locked iPhone is essentially worthless except for spare parts.

Six victims shared their experiences with the NY Times. Experts say the threatening texts follow a clear, copy-and-paste pattern — deception first, fake sympathy second, violent threats third. Some gangs appear to use identical language across victims, suggesting an organized, industrial-scale operation.

Why the Threats Work (Even Though They're Fake)

Criminologists explain the psychology: victims have lost one of their most personal and expensive possessions, and the criminals are threatening to weaponize everything on it — emails, bank info, private photos. As one expert put it, it becomes a "multifaceted psychological attack." The threats of physical violence are almost certainly empty — committing violence overseas over a single phone makes no sense — but the emotional toll is real. And the math works for criminals: even if only a small fraction of victims comply and unlink their devices, it's well worth the negligible effort of sending a text.

Not everyone gives in. Christopher Bramah-Calvert, another victim, and his husband received the same gun video and death threats and dismissed them as "ridiculous" — though he acknowledged most people would feel more intimidated.

What Apple and Authorities Are Doing

London Mayor Sadiq Khan and Metropolitan Police Commissioner Mark Rowley have publicly pushed Apple to go further — specifically asking why there isn't a remote "kill switch" that makes a stolen phone permanently useless, or a way to deny cloud access once a device is reported stolen.

Apple responded that it already offers Lost Mode, remote erasing, and keeping the device on the Find My list to prevent reactivation, and pledged to "continue to work tirelessly to reduce the incentives for stealing Apple devices."

On the legal side, the threats could technically be prosecuted under British law as "malicious communications," carrying up to a two-year jail sentence — but only if sent from British soil. Since the messages originate in China or the Philippines, British police acknowledge there is very little they can actually do.

The Bottom Line

Experts and police unanimously advise victims: **do not unlink your Apple ID.** Wipe the phone remotely, keep it in Lost Mode, and ignore the threats — they are almost certainly coming from overseas criminals who have no ability to follow through. The goal is purely psychological pressure to extract a quick, easy profit.